

FIG. 1  
(PRIOR ART)

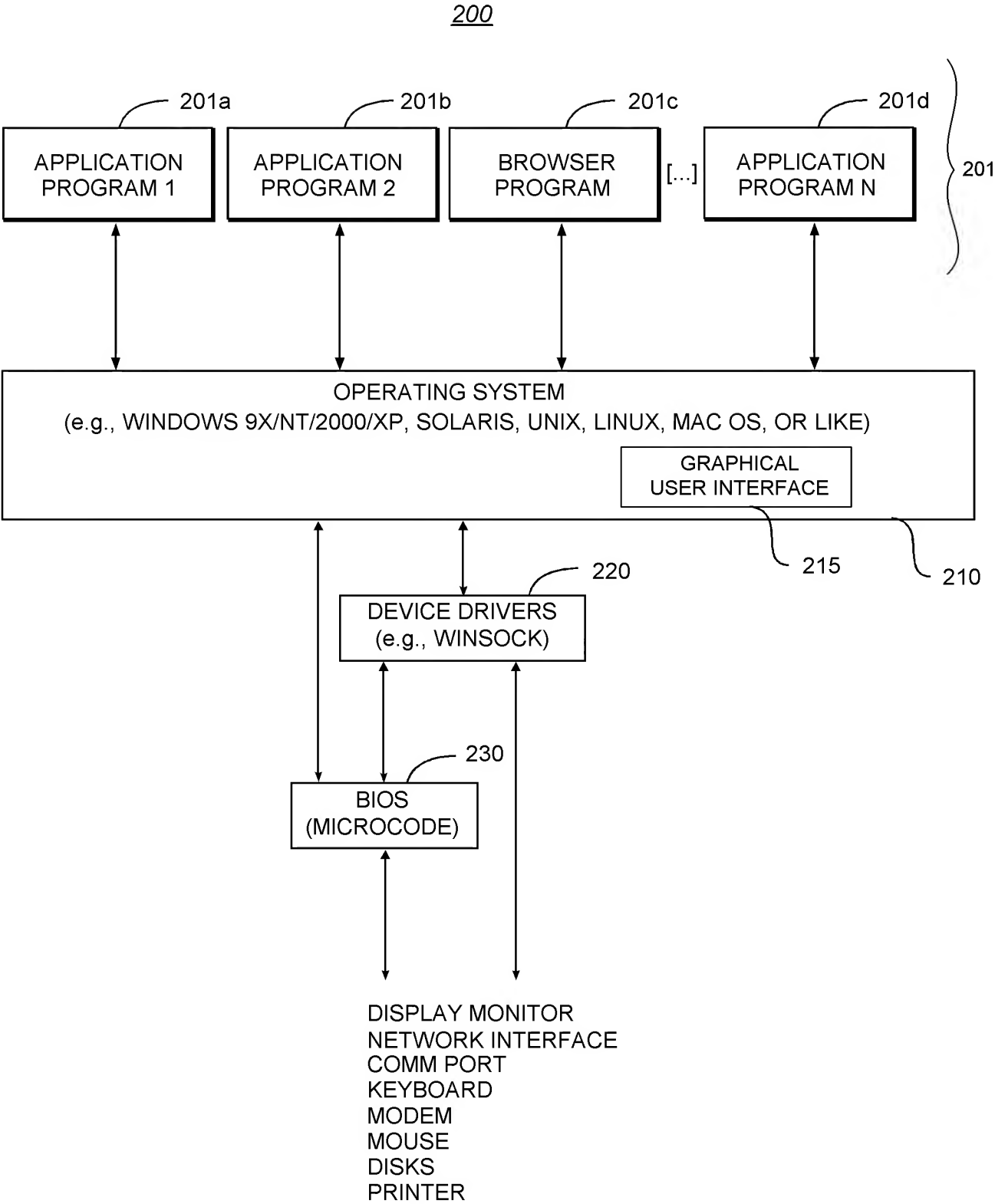
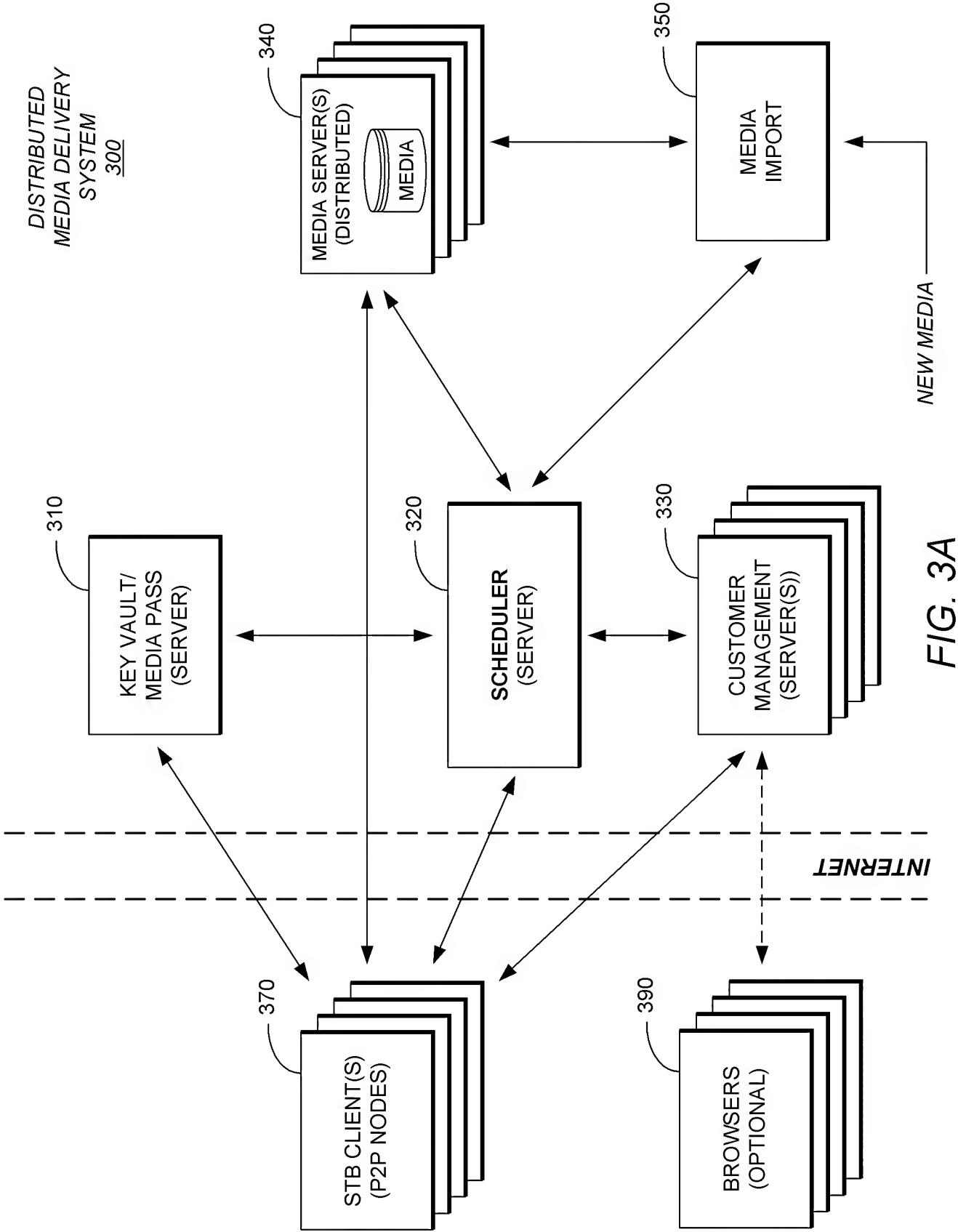


FIG. 2



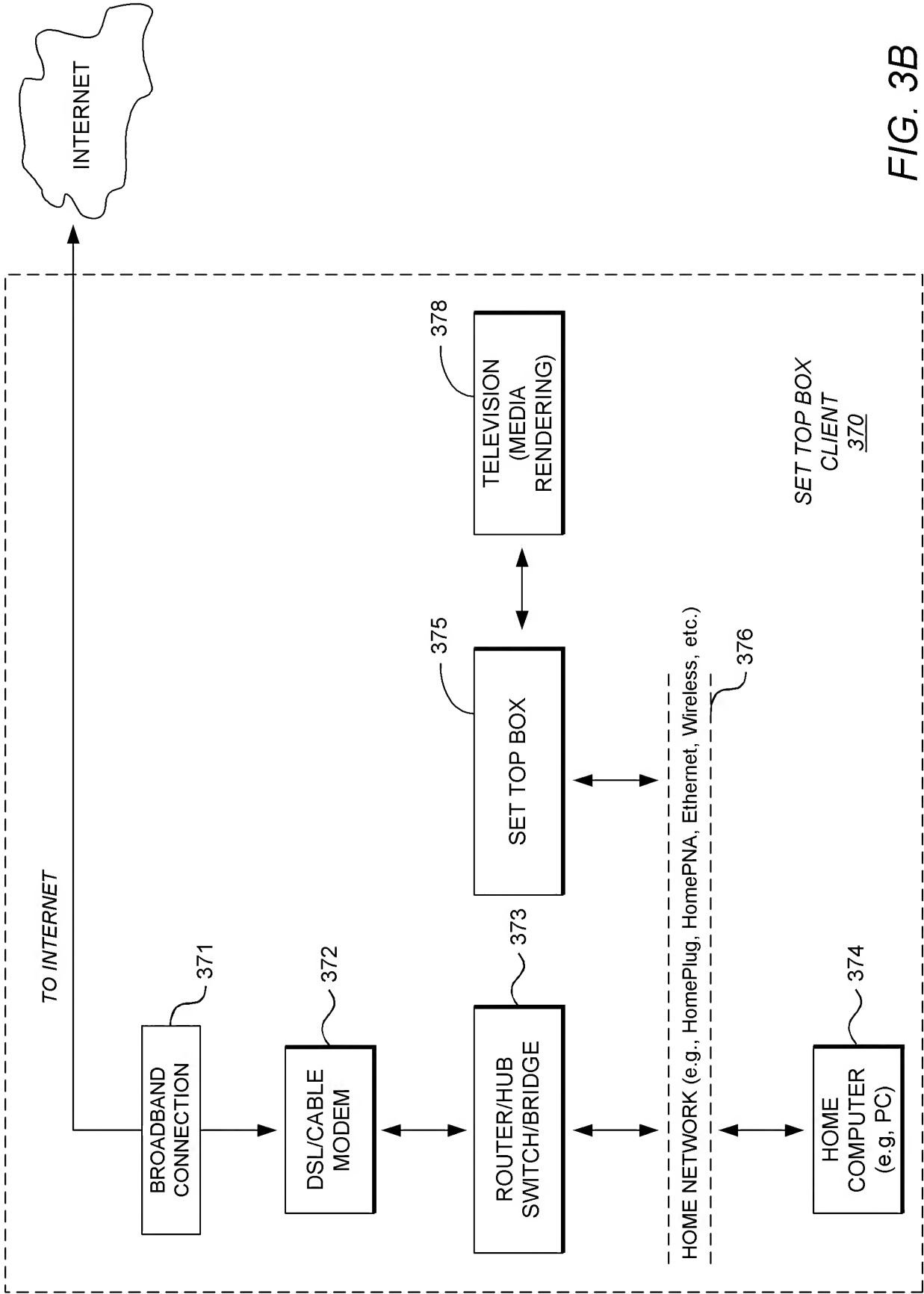


FIG. 3B

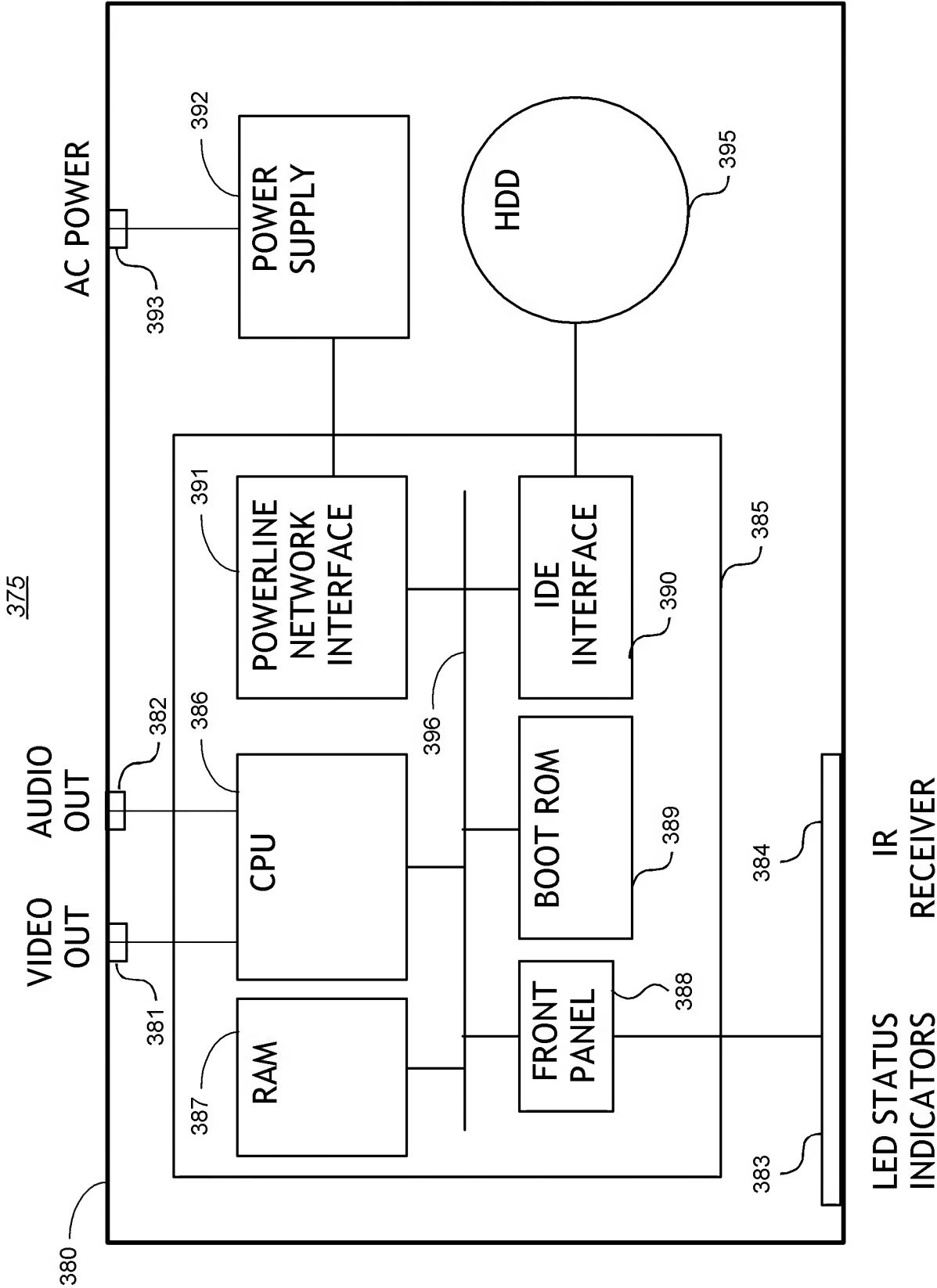


FIG. 3C

NEW USER

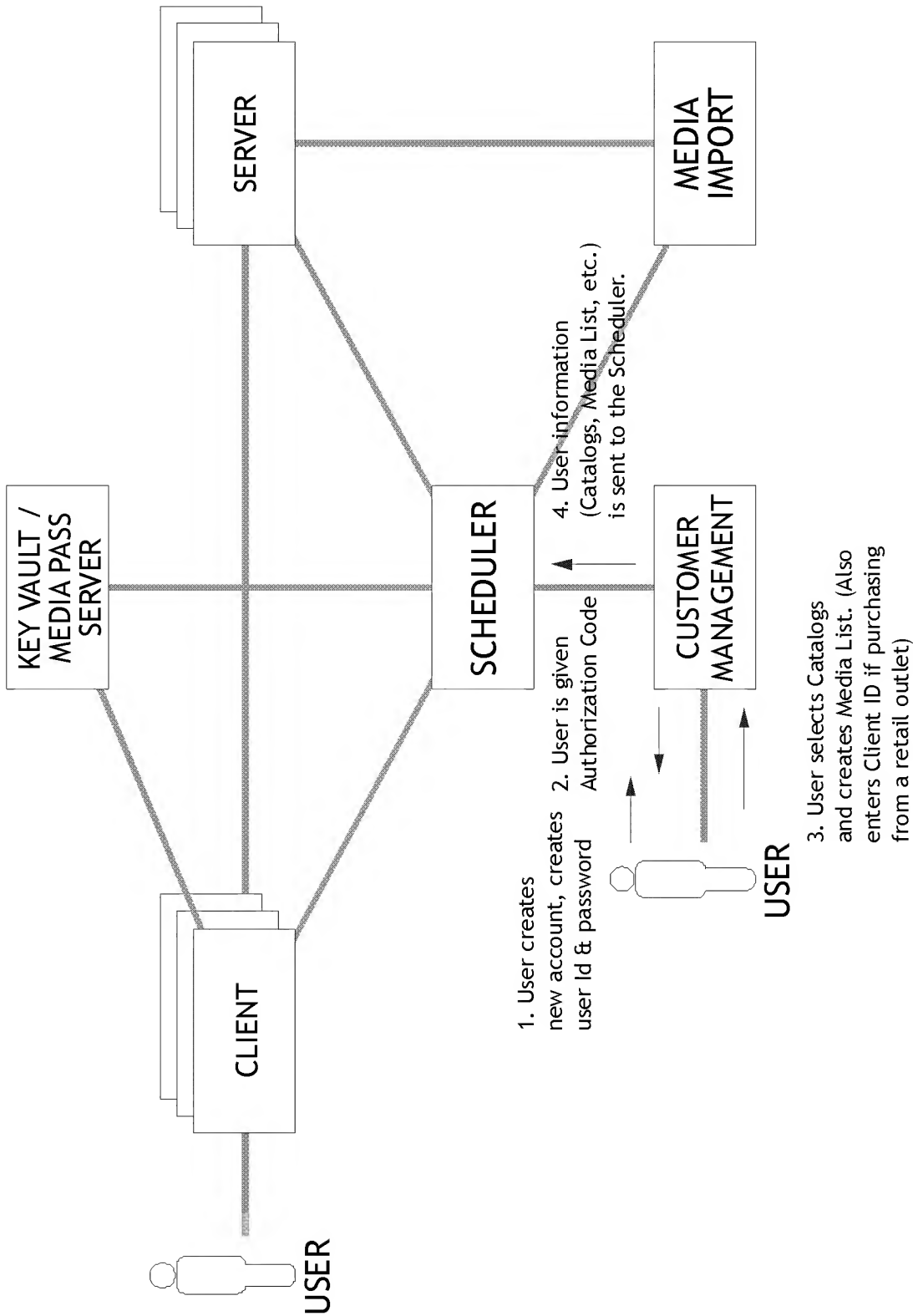


FIG. 4

NEW CLIENT

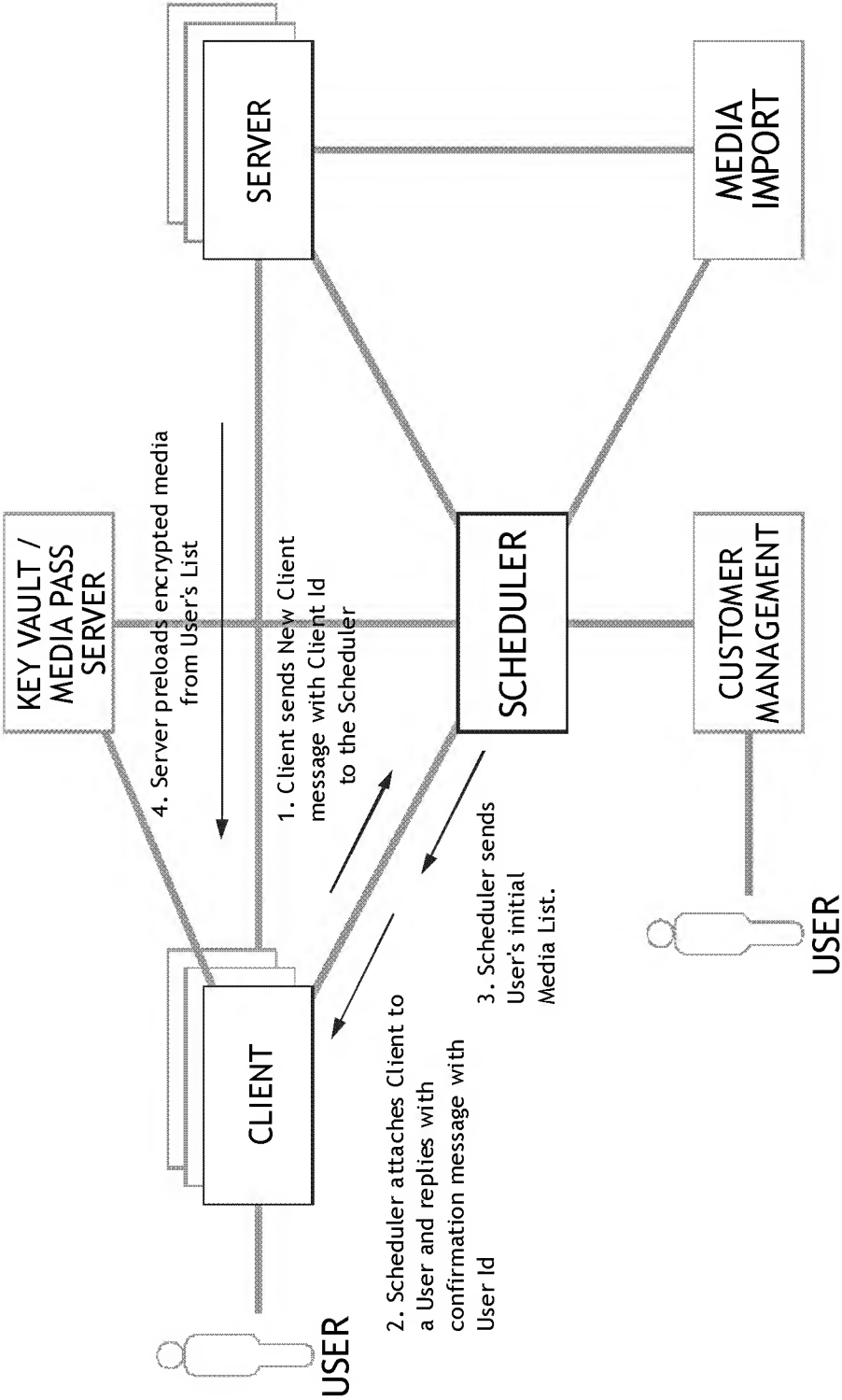


FIG. 5

USER RECEIVES CLIENT

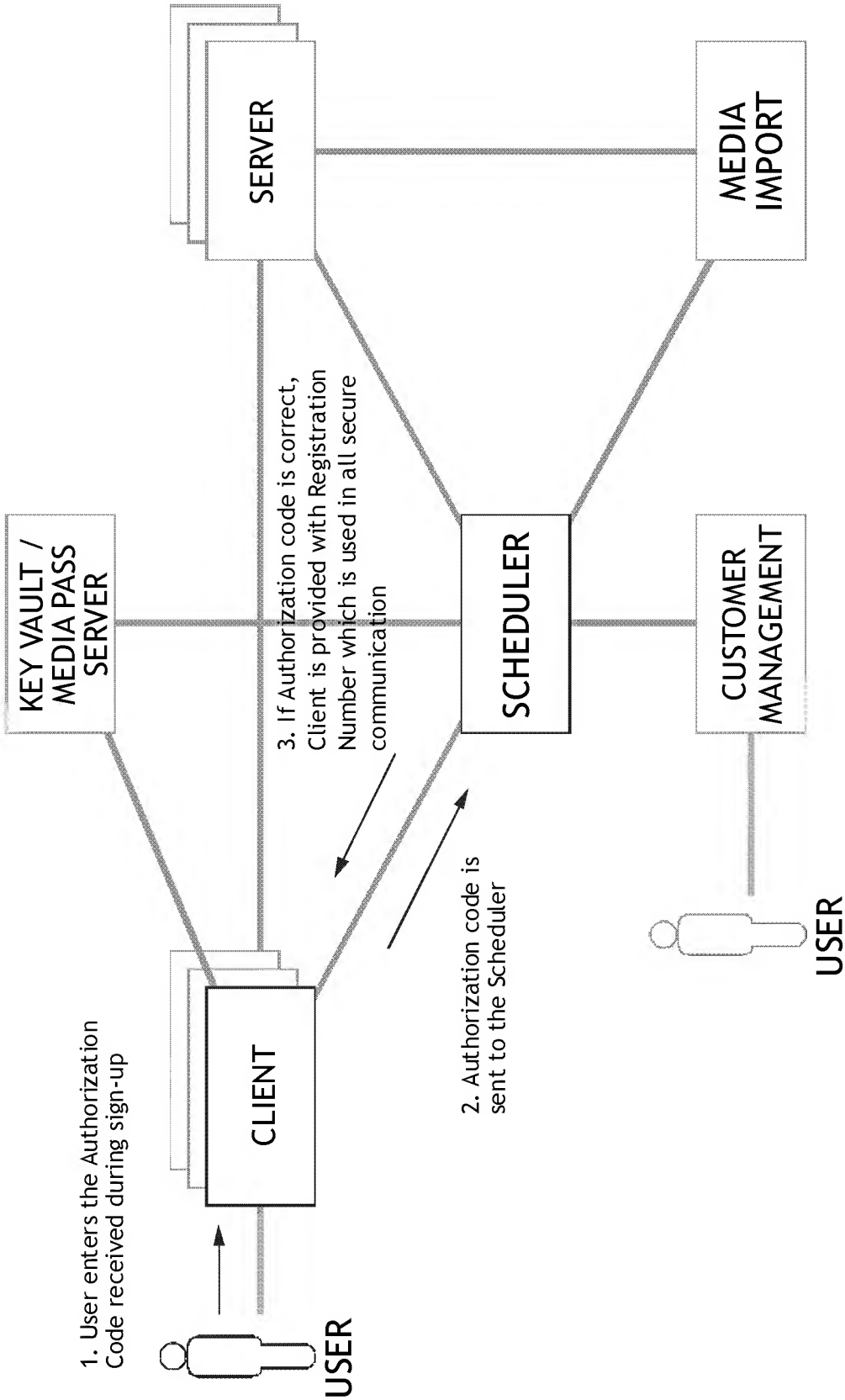


FIG. 6



NEW MEDIA

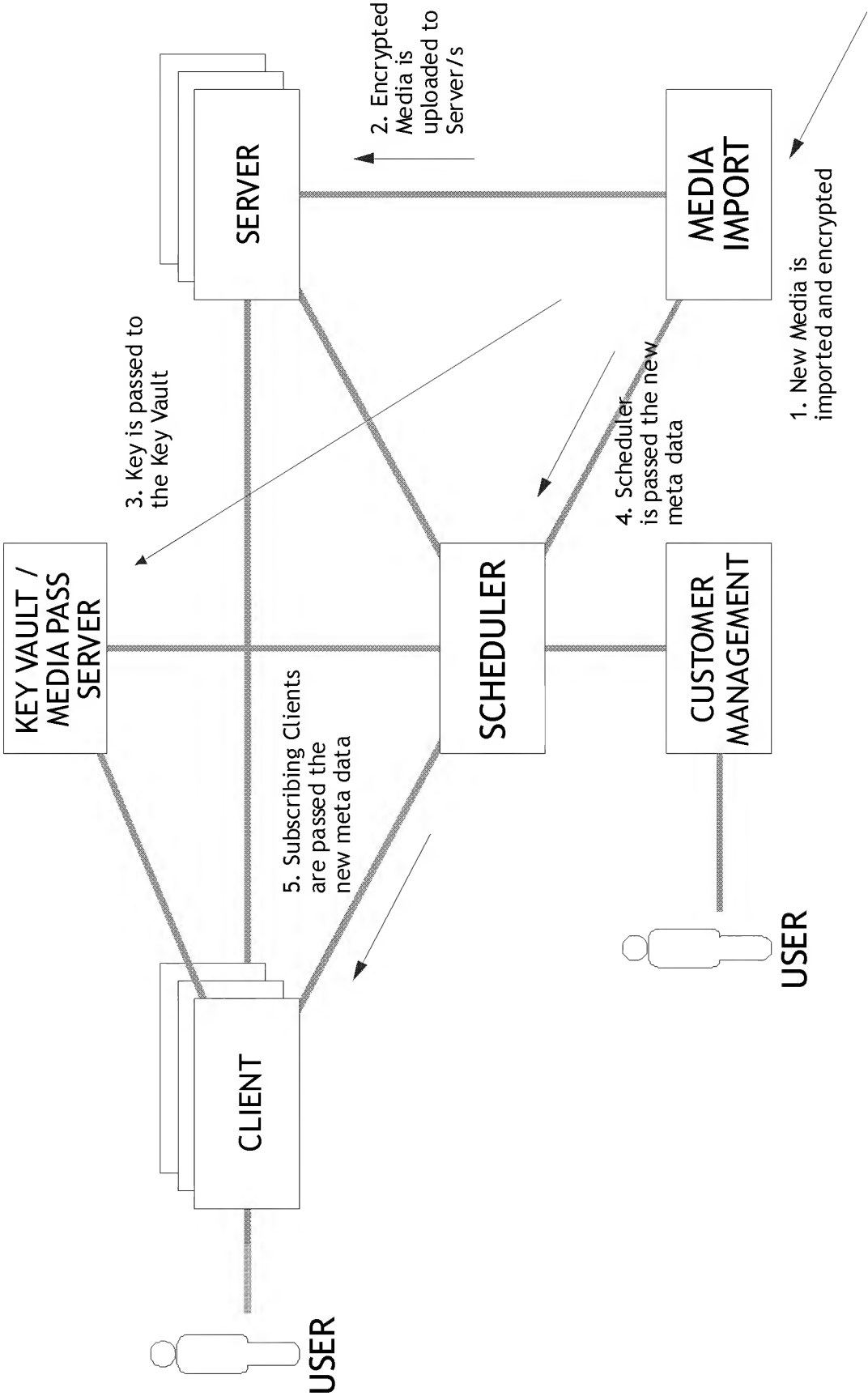


FIG. 7

USER ADDS MEDIA TO LIST

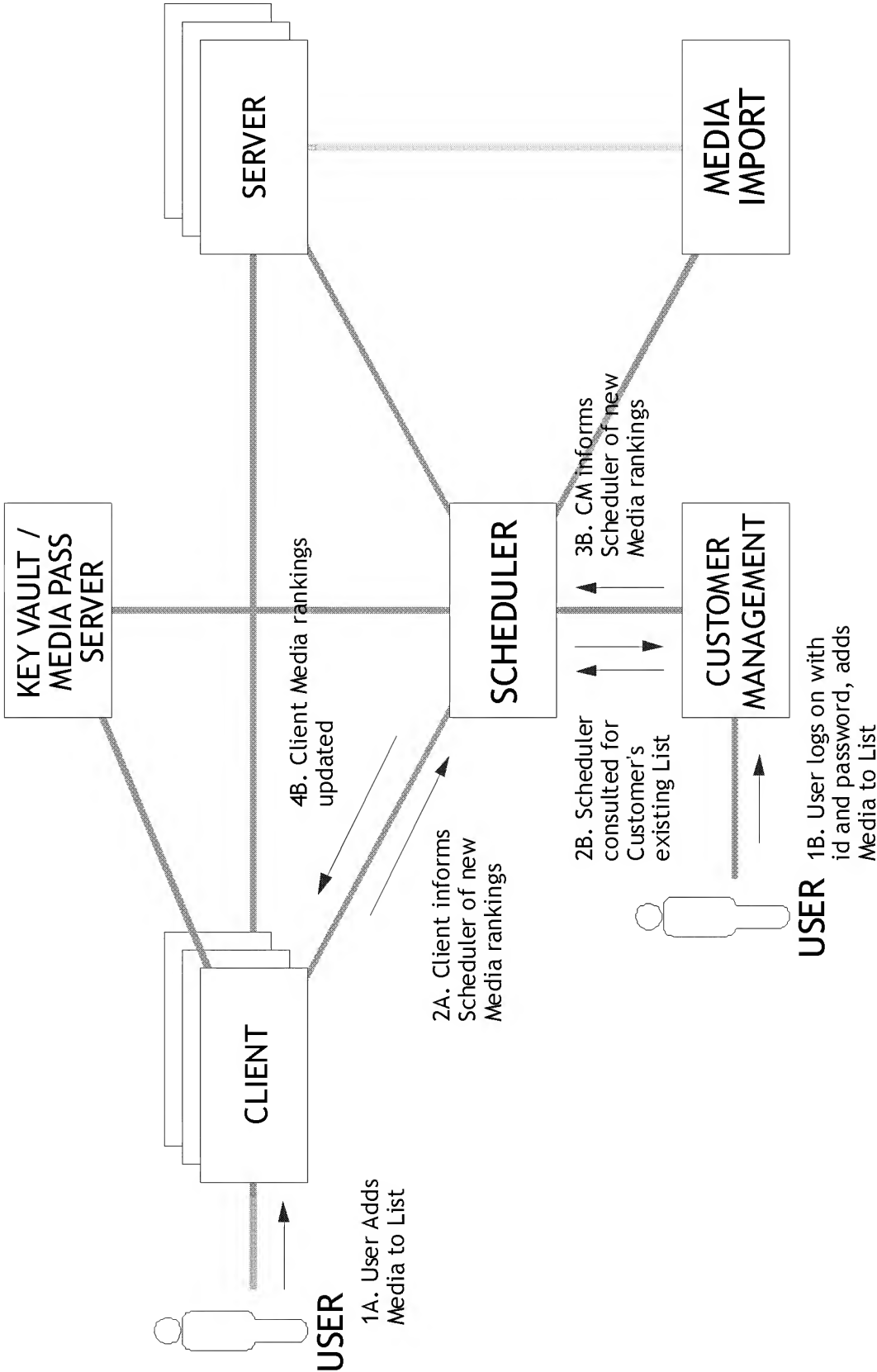


FIG. 8A

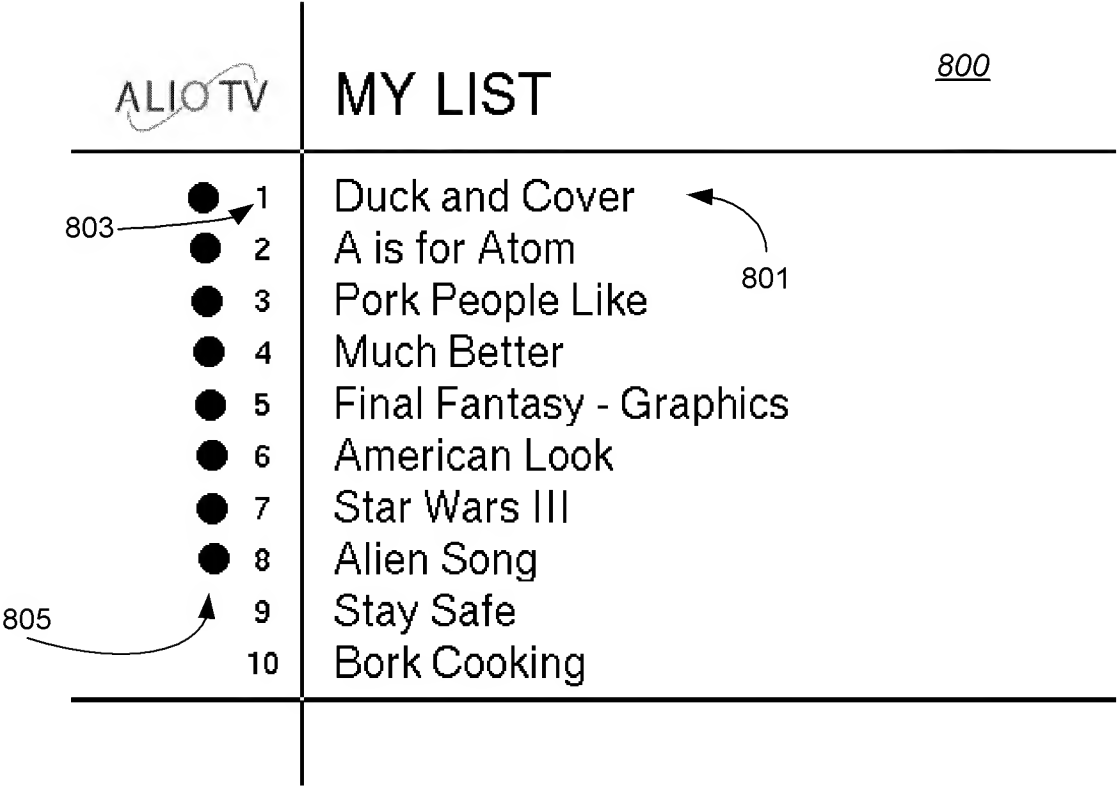


FIG. 8B



FIG. 8C

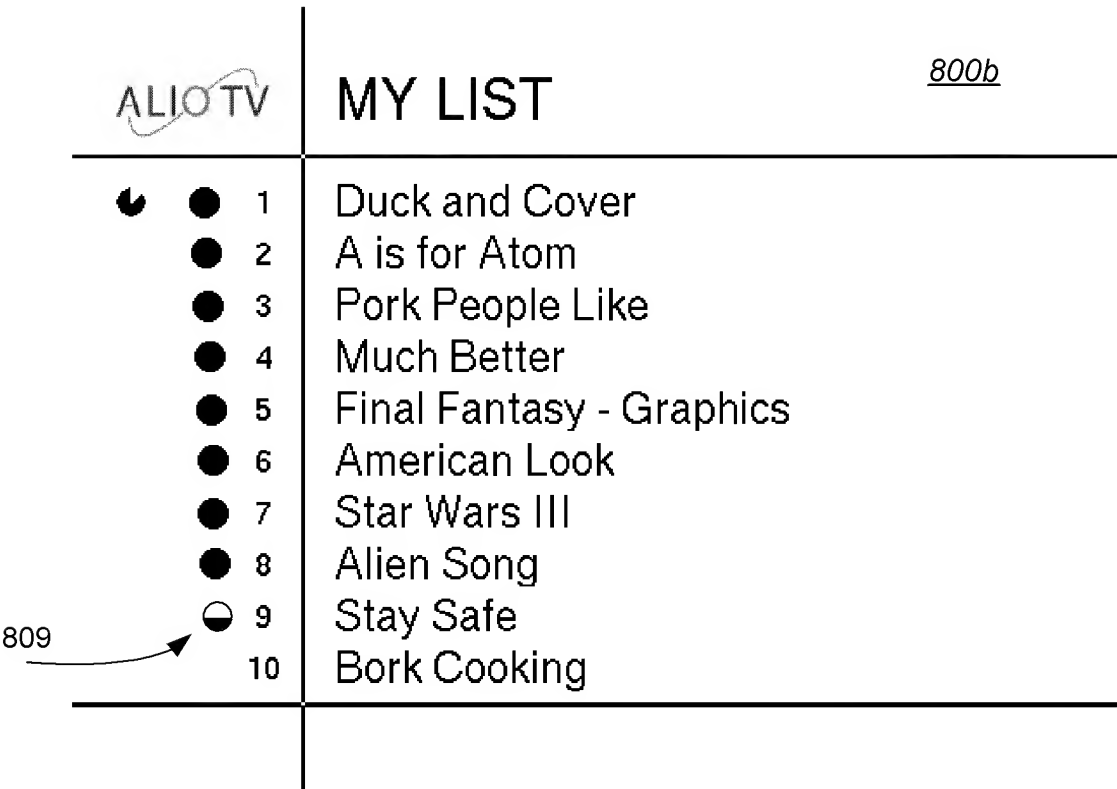


FIG. 8D

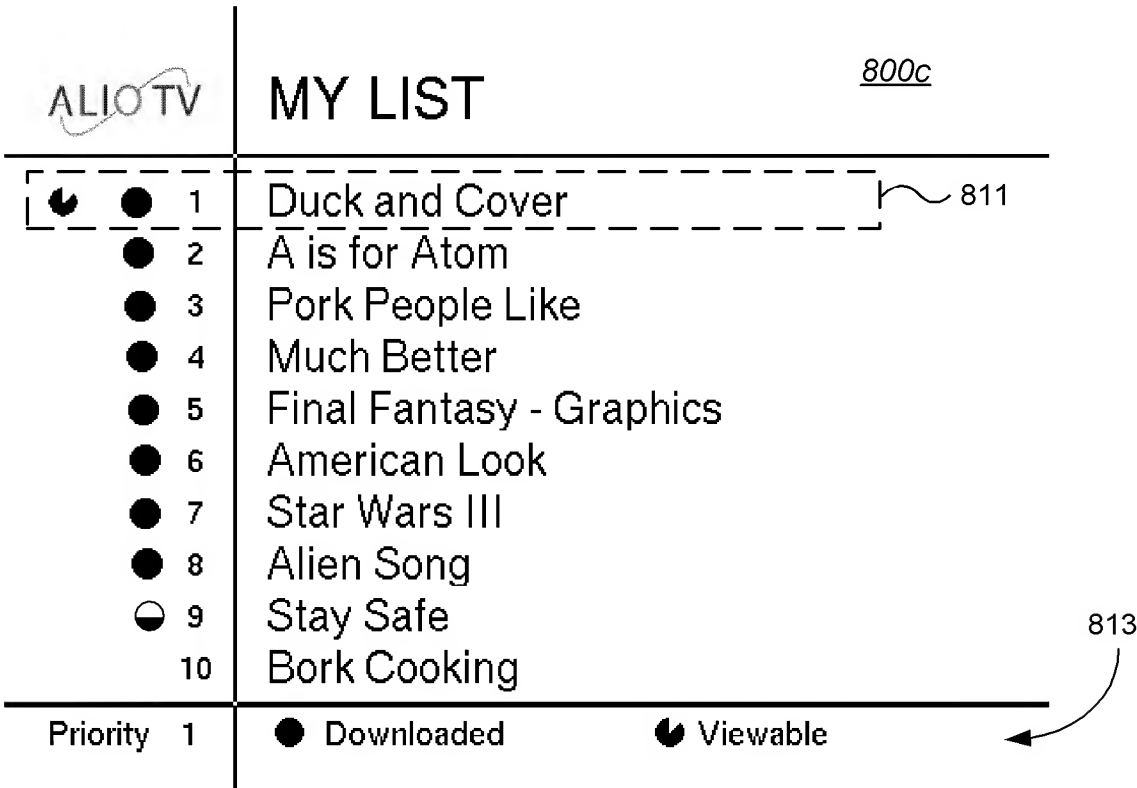


FIG. 8E

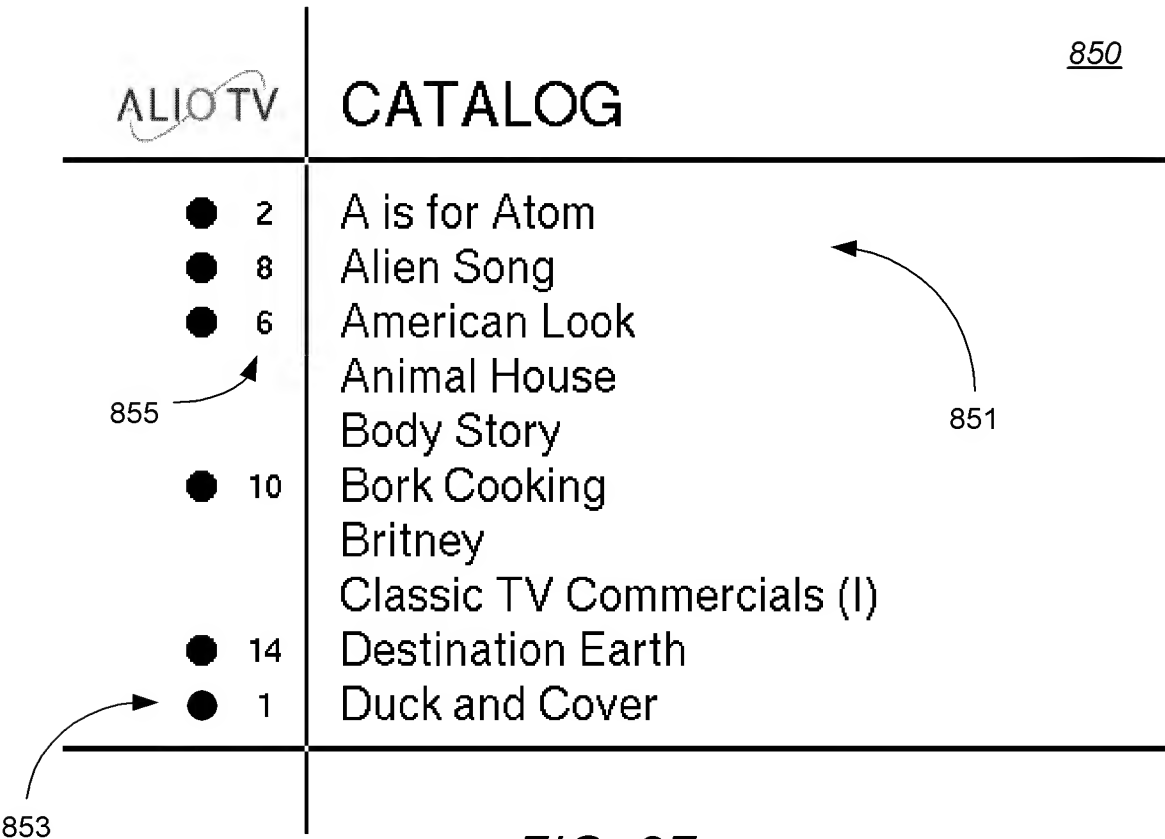


FIG. 8F

USER RE-ARRANGES LIST

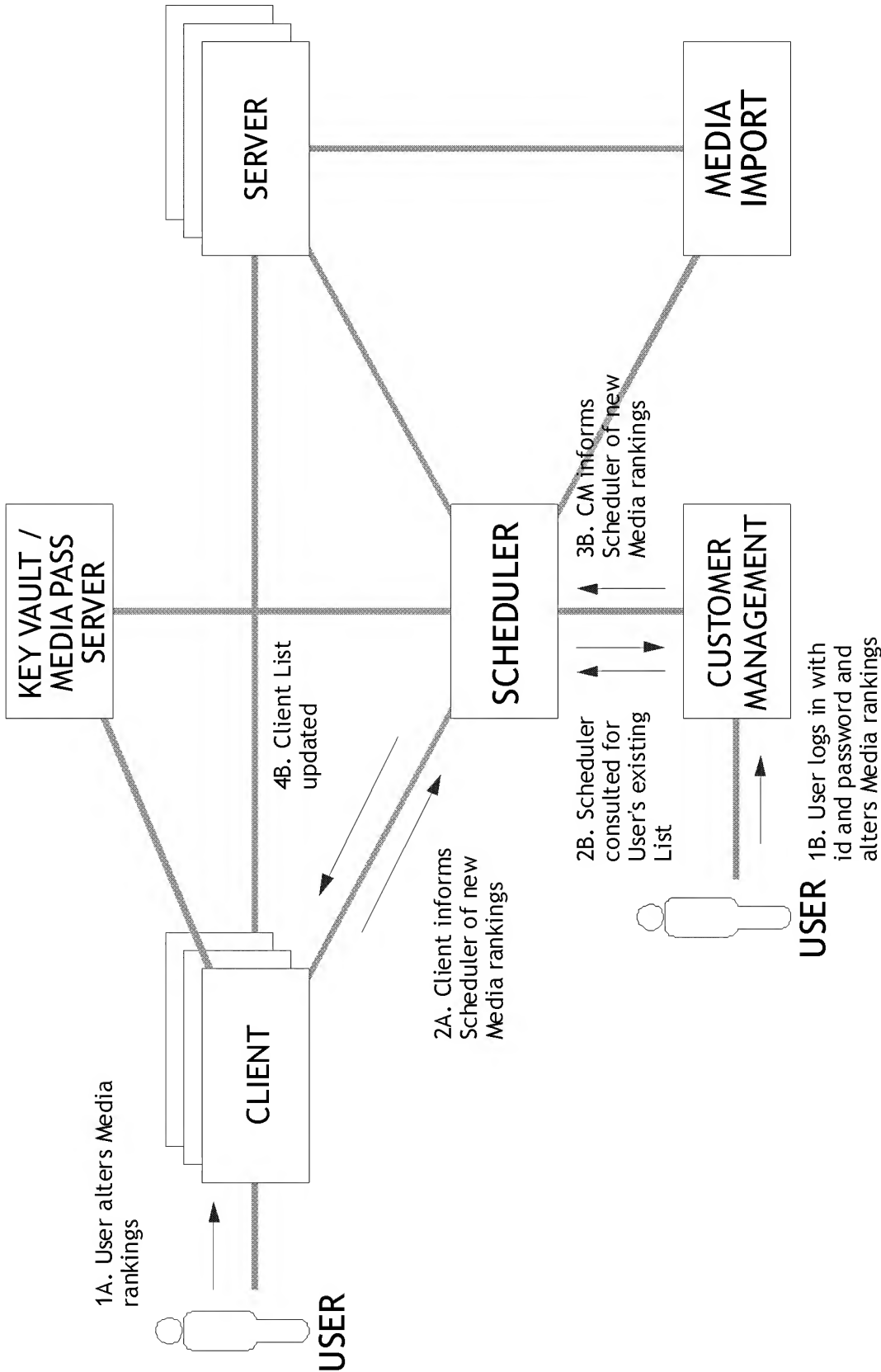


FIG. 9

MEDIA TRANSFER

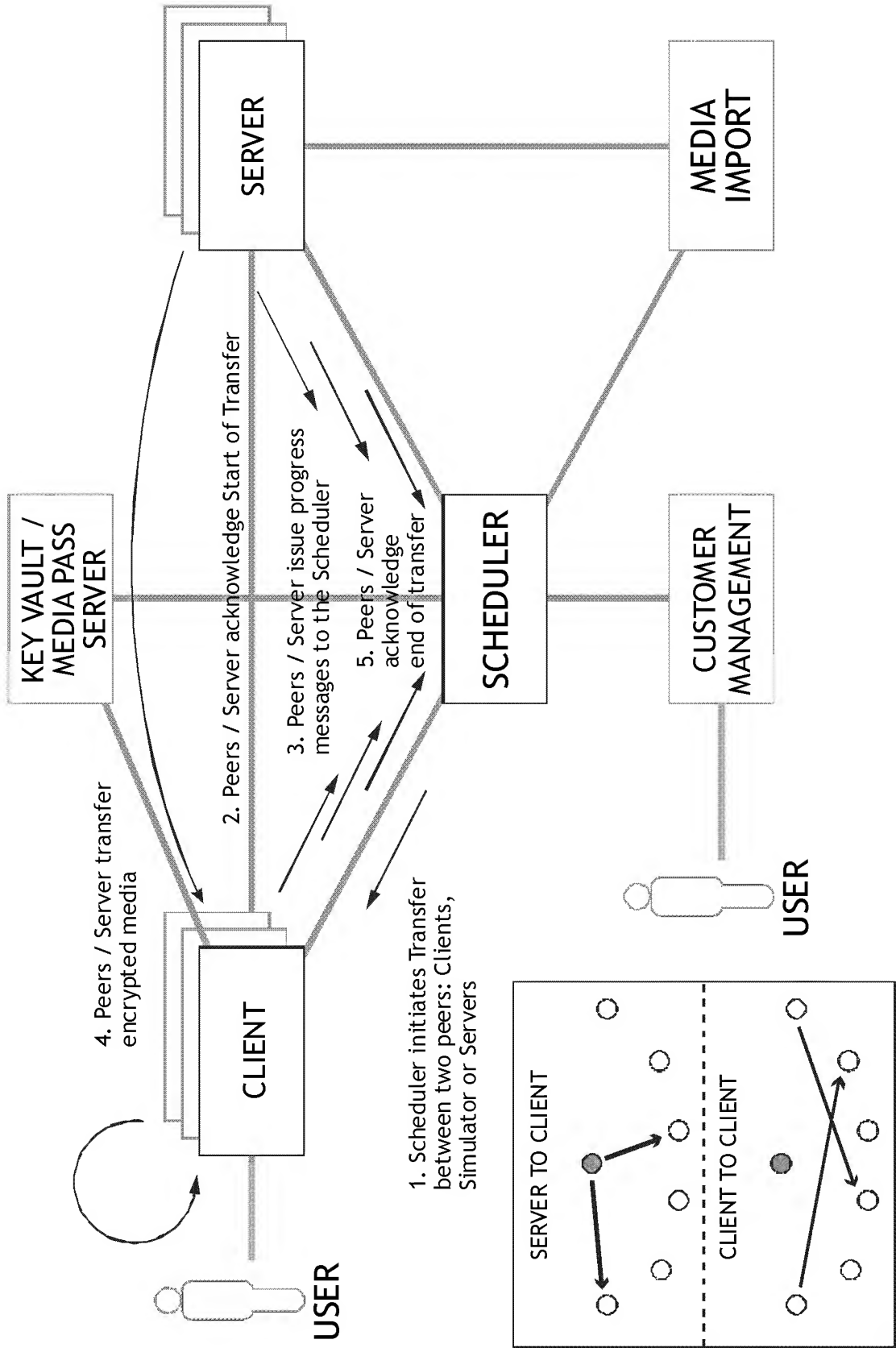


FIG. 10

USER REQUESTS MOVIE PURCHASE

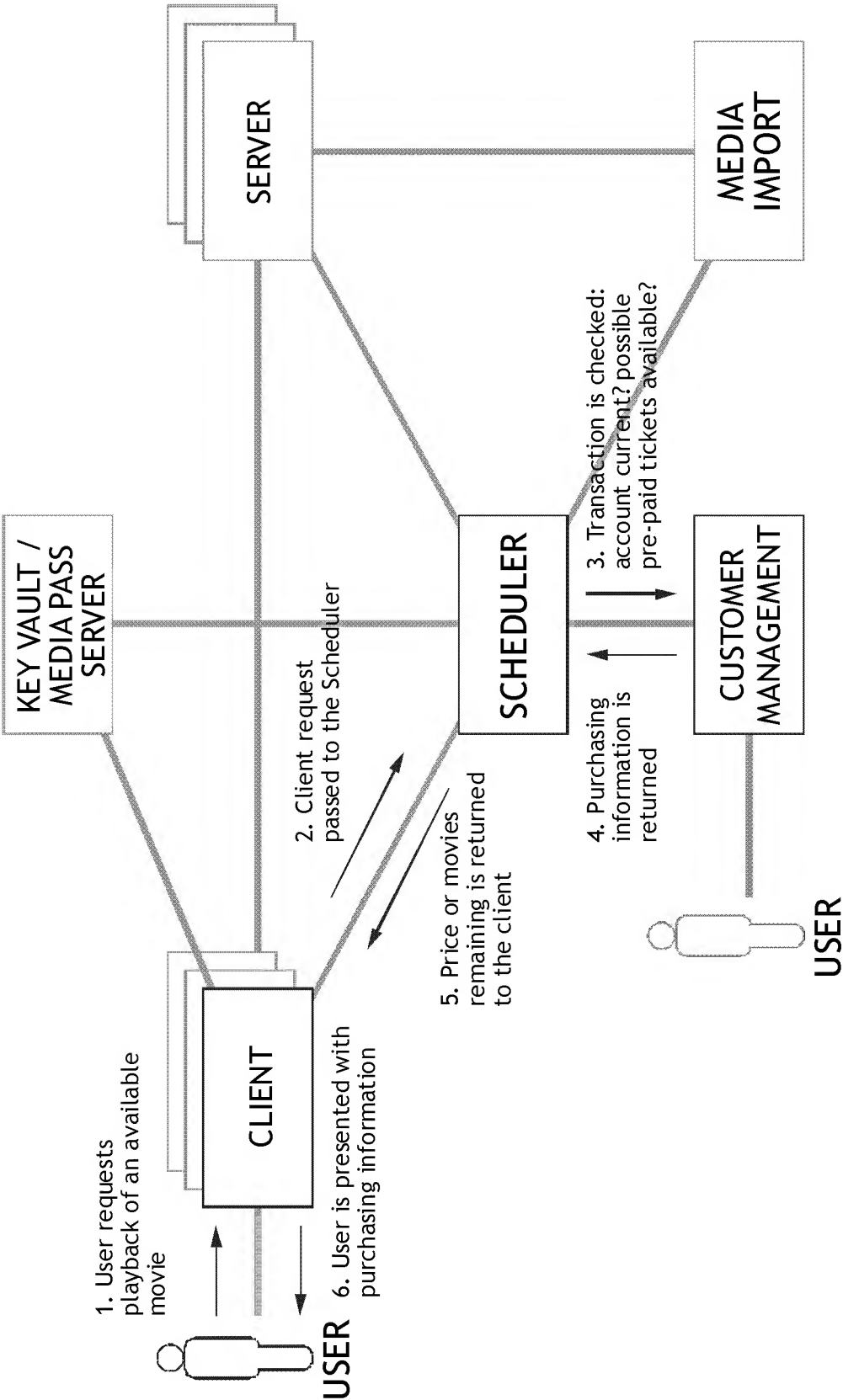


FIG. 11



PLAYBACK

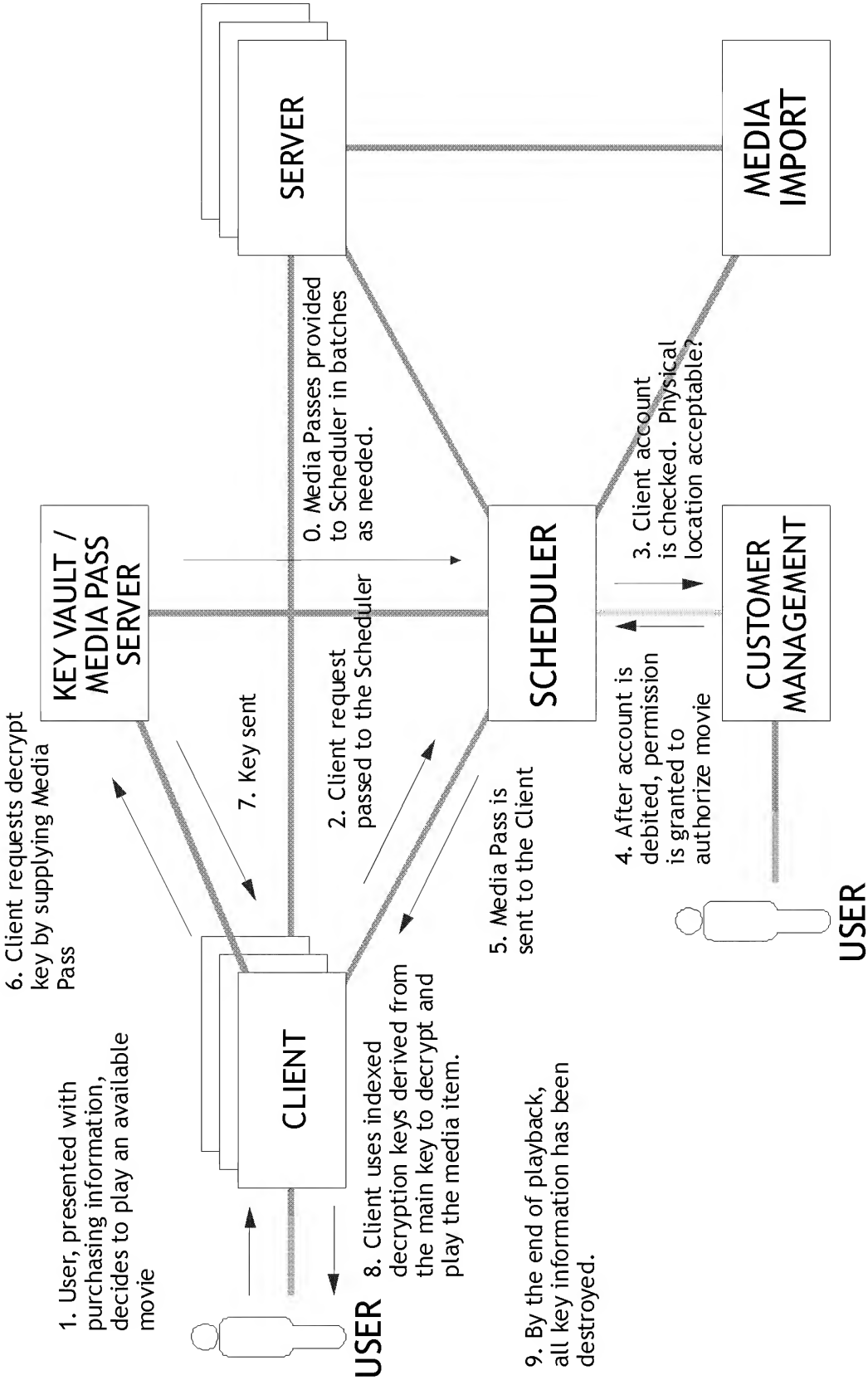
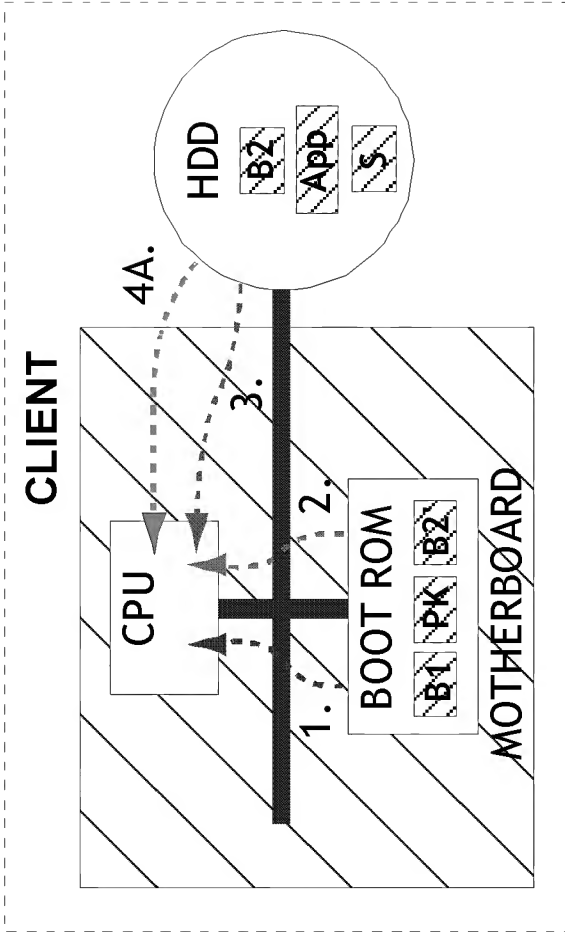


FIG. 12

SECURE CLIENT - BOOT PROCESS



1. Initial Stage I  
Boot (B1) from  
Boot ROM

2. Public Key  
(PK) read from  
BOOT ROM

3. HDD Code Image (B2  
& App) signature (S) is  
verified with public key  
(PK)

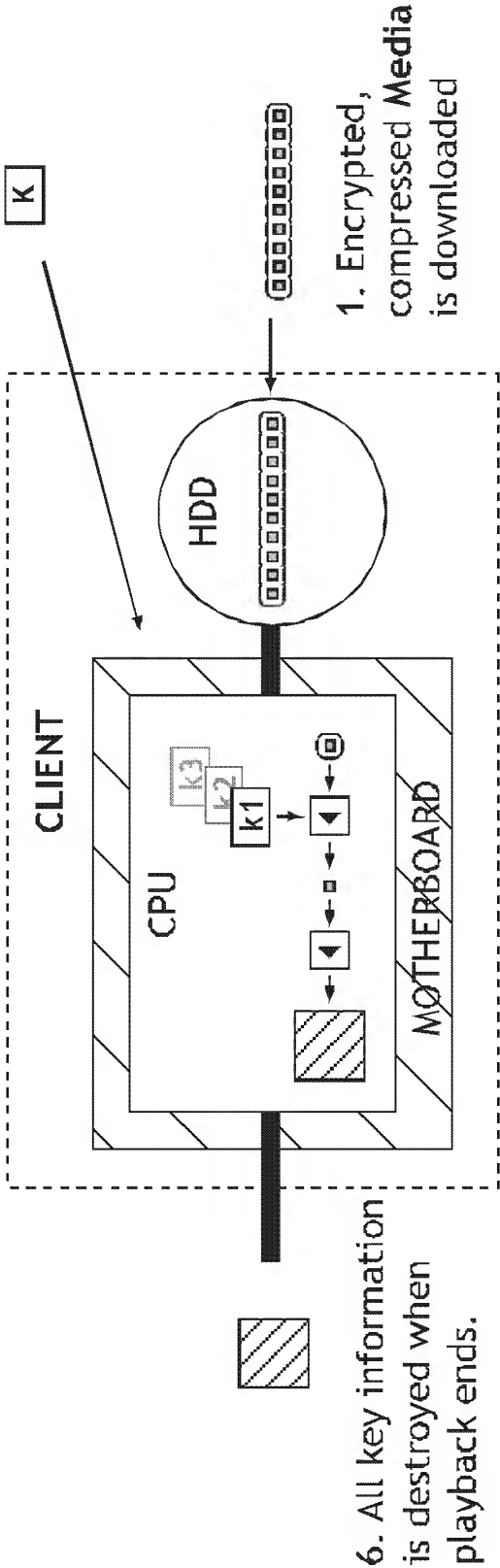
4A. If signature is verified, Stage II boot  
(B2) continues from HDD, application  
execution (App) commences.

4B. If signature does not verify, fallback  
code (B2') is used from Boot ROM.  
System will require service.

FIG. 13

SECURE CLIENT - PLAYBACK

3. After the Media Pass negotiation, **Key (K)** is delivered to the **Client**



1. Encrypted, compressed **Media** is downloaded

2. Media is stored on HDD

4. Media is decrypted frame by frame with indexed decryption keys (k1, k2, k3, ...)

5. Each frame is decompressed (on-chip SW or HW). Decrypted, compressed media *never* appears outside CPU

PLAYBACK

FIG. 14

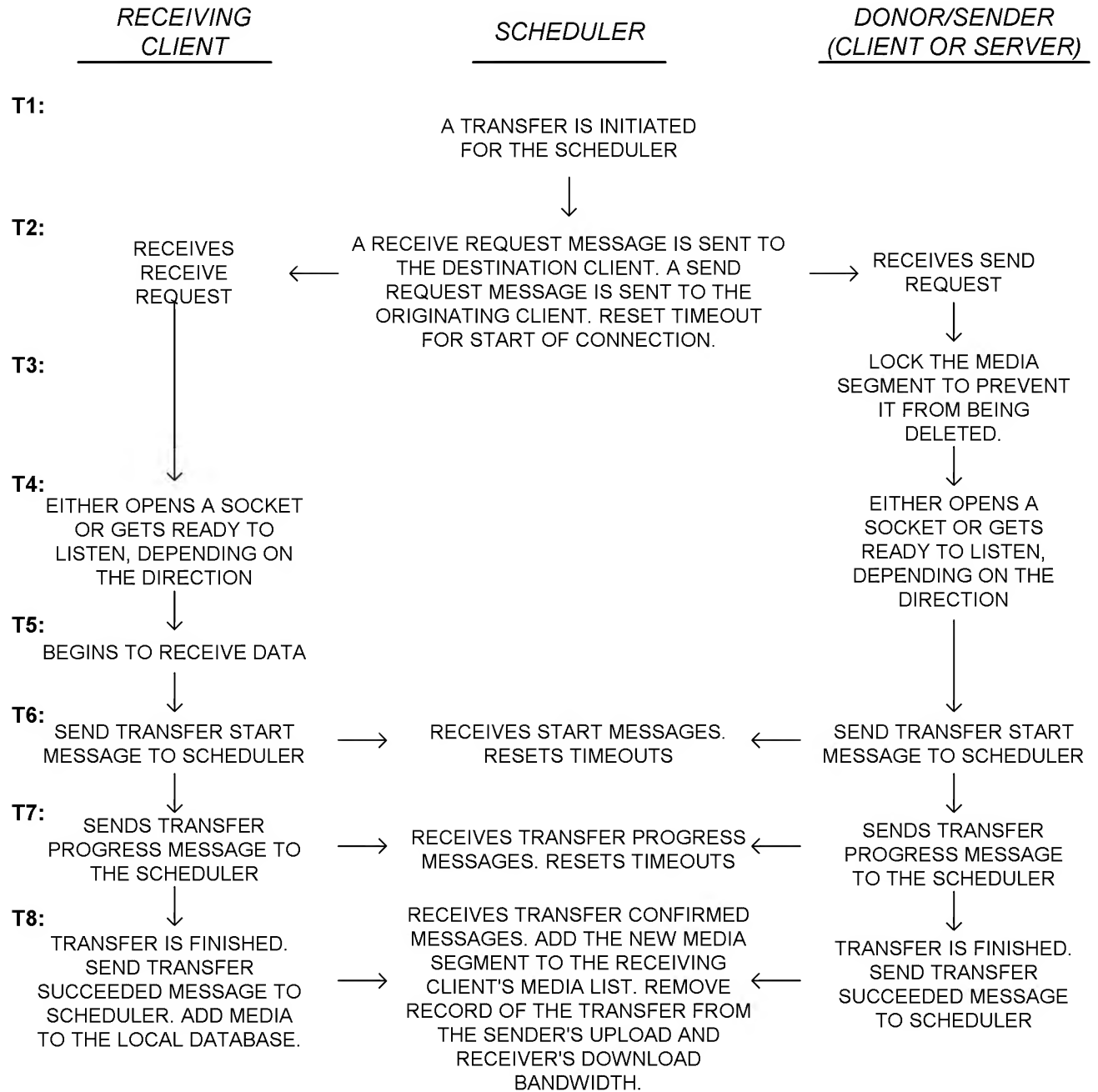
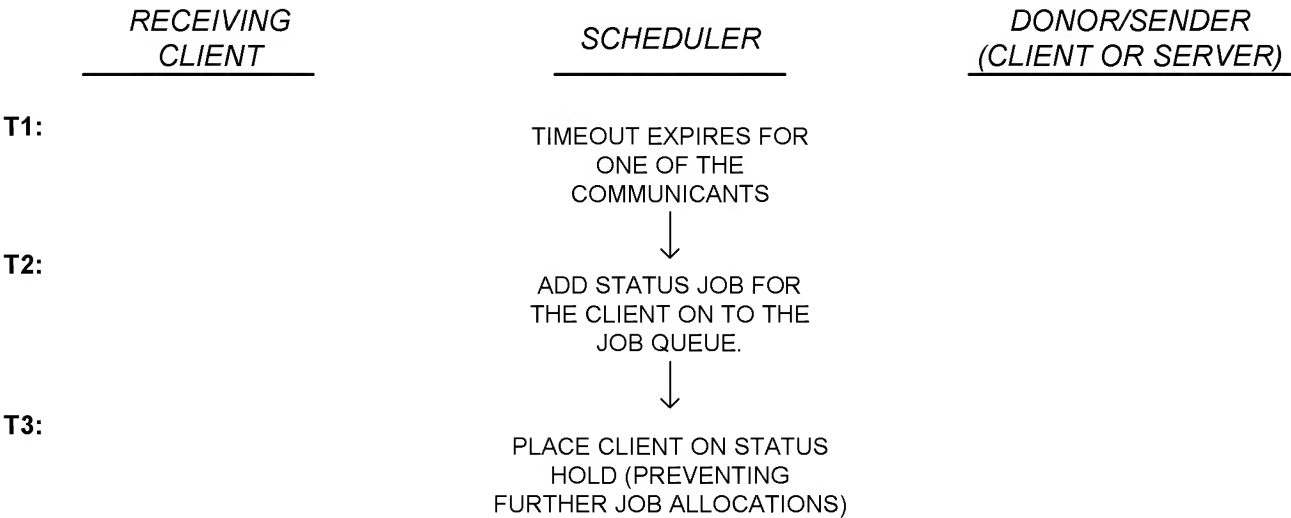


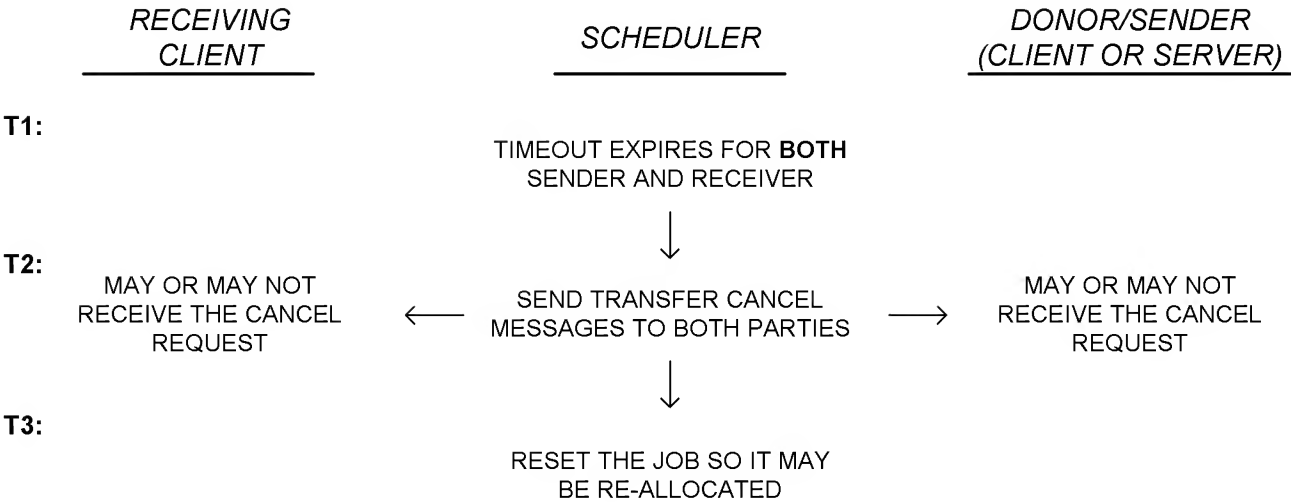
FIG. 15A

**ONE TIMES OUT**

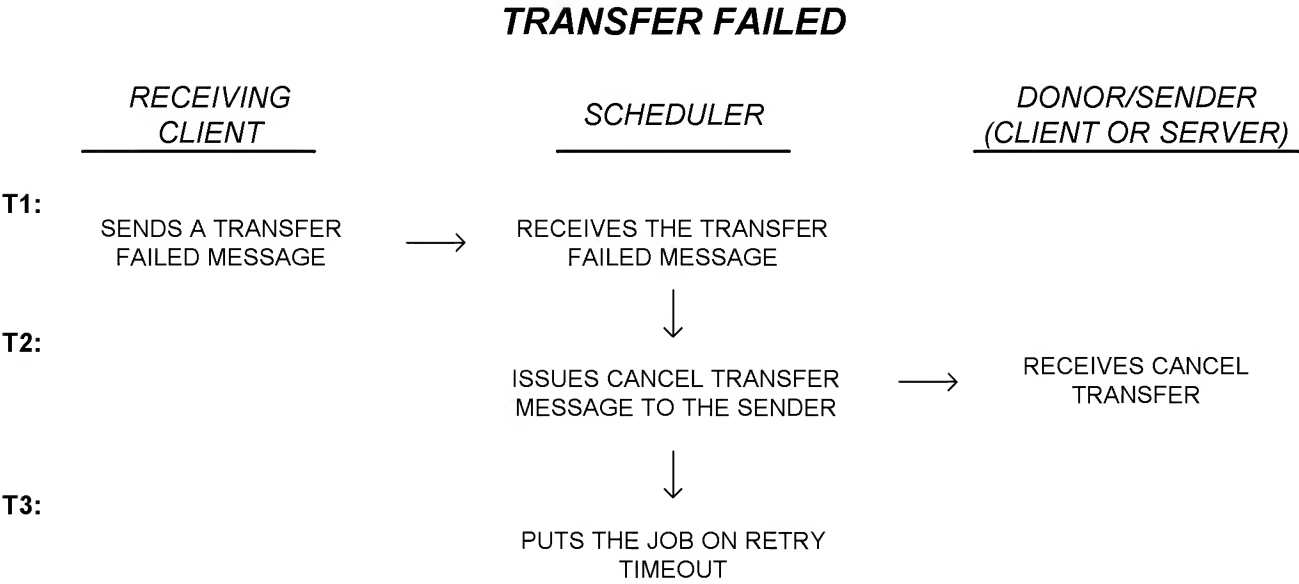


**FIG. 15B**

**BOTH TIME OUT**



**FIG. 15C**



*FIG. 15D*